Coverings of curves with asymptotically many rational points *

Wen-Ching W Li and Hiren Maharaj

Department. of Mathematics
Pennsylvania State University
University Park, PA 16802-6401
wli@math.psu.edu, maharaj@math.psu.edu

25 August 1999

Abstract

The number $A(q)$ is the upper limit of the ratio of the maximum number of points of a curve defined over $\mathbb{F}_q$ to the genus. By constructing class field towers with good parameters we present improvements of lower bounds of $A(q)$ for q an odd power of a prime.

1 Introduction

Given a finite field $\mathbb{F}_q$ of q elements, by $K/\mathbb{F}_q$ we mean a global function field K with full constant field $\mathbb{F}_q$, that is, with $\mathbb{F}_q$ algebraically closed in K. A *rational place* of K is a place of K of degree 1. Write $N(K)$ for the number of rational places of K and $g(K)$ for the genus of K. According to the Weil-Serre bound (see [16], [17]) we have

$$N(K) \leq q + 1 + g(K)\lfloor 2q^{1/2} \rfloor, \tag{1}$$

where $\lfloor t \rfloor$ is the greatest integer not exceeding the real number t.

Definition 1.1 *For any prime power q and any integer $g \geq 0$ put*

$$N_q(g) = \max N(K),$$

where the maximum is extended over all global function fields K of genus g with full constant field $\mathbb{F}_q$.

In other words, $N_q(g)$ is the maximum number of $\mathbb{F}_q$-rational points that a smooth, projective, absolutely irreducible algebraic curve over $\mathbb{F}_q$ of genus g can have. The following quantity was introduced by Ihara [7].

Definition 1.2 *For any prime power q let*

$$A(q) = \limsup_{g\to\infty} \frac{N_q(g)}{g}.$$

*Research supported in part by the NSF grants DMS96-22938 and DMS99-70651.

It follows from (1) that $A(q) \le \lfloor 2q^{1/2} \rfloor$. Furthermore, Ihara [7] showed that $A(q) \ge q^{1/2} - 1$ if q is a square. In the special cases $q = p^2$ and $q = p^4$, this lower bound was also proved by Tsfasman, Vlădut, and Zink [20]. Hereafter, p always denotes a prime number. Vlădut and Drinfel'd [21] established the bound

$$A(q) \le q^{1/2} - 1 \tag{2}$$

for all q. In particular this yields that $A(q) = q^{1/2} - 1$ if q is a square. Garcia and Stichtenoth [1], [3] proved that if q is a square, then $A(q) = q^{1/2} - 1$ can be achieved by an explicitly constructed tower of global function fields.

In the case where q is not a square, no exact values of $A(q)$ are known, but lower bounds are available which complement the general upper bound (2). According to a result of Serre [16], [17] (see also [11]) based on class field towers, we have

$$A(q) \ge c \log q \tag{3}$$

with an absolute constant $c > 0$. Zink [22] gave the best known lower bound for p^3:

$$A(p^3) \ge \frac{2(p^2-1)}{p+2}. \tag{4}$$

Later, Perret [13] proved that if l is a prime and if $q > 4l + 1$ and $q \equiv 1 \bmod l$, then

$$A(q^l) \ge \frac{l^{1/2}(q-1)^{1/2} - 2l}{l-1}. \tag{5}$$

Niederreiter and Xing [10] generalised and improved (5) by establishing the following bounds. If q is odd and $m \ge 3$ is an integer, then

$$A(q^m) \ge \frac{2q}{\lceil 2(2q+1)^{1/2} \rceil + 1}. \tag{6}$$

If $q \ge 4$ is even and $m \ge 3$ is an odd integer, then

$$A(q^m) \ge \frac{q+1}{\lceil 2(2q+2)^{1/2} \rceil + 2}. \tag{7}$$

As a consequence, they improved the Gilbert-Varshamov bound for sufficiently large composite nonsquare q on a certain interval. Furthermore in [10] they showed that $A(2) \ge \frac{81}{317} = 0.2555\ldots$, $A(3) \ge \frac{62}{163} = 0.3803\ldots$ and $A(5) \ge \frac{2}{3} = 0.666\ldots$.

Denote the number of places of degree r in a function field F by $B_r(F)$ or simply B_r if there is no danger of confusion. Niederreiter and Xing further extended their bounds (6) and (7) to the following result in [11].

Theorem 1.3 *Let $F/\mathbb{F}_q$ be a global function field with $N \ge 1$ rational places. Let $r \ge 3$ be an integer. Suppose that the ratio of class numbers $h(F\mathbb{F}_{q^r})/h(F)$ is odd.*
(1) *If q is odd and $B_r(F) \ge 2(2N-1)^{1/2} + 3$, then*

$$A(q^r) \ge \frac{2(N-1)}{2g(F) + \lceil 2(2N-1)^{1/2} \rceil + 1}. \tag{8}$$

(2) *If q is even and $B_r(F) \ge 2(2N-2)^{1/2} + 3$, then*

$$A(q^r) \ge \frac{N-1}{g(F) + \lceil 2(2N-2)^{1/2} \rceil + 2}. \tag{9}$$

The bounds (6) and (7) follow from the above theorem by considering the rational function field over $\mathbb{F}_q$. Using this theorem, they also found improved lower bounds for $A(q^3)$:

Corollary 1.4 (1) *If q is a power of an odd prime p and p does not divide $\lfloor 2q^{1/2} \rfloor$, then*

$$A(q^3) \geq \frac{2q + 4\lfloor q^{1/2} \rfloor}{3 + \lceil 2(2q + 4\lfloor q^{1/2} \rfloor + 1)^{1/2} \rceil}. \tag{10}$$

If q is odd and p divides $\lfloor 2q^{1/2} \rfloor$, then

$$A(q^3) \geq \frac{2q + 4\lfloor q^{1/2} \rfloor - 4}{3 + \lceil 2(2q + 4\lfloor q^{1/2} \rfloor - 3)^{1/2} \rceil}. \tag{11}$$

(2) *If $q \geq 4$ is even and $\lfloor 2q^{1/2} \rfloor$ is odd, then*

$$A(q^3) \geq \frac{q + \lfloor 2q^{1/2} \rfloor}{3 + \lceil 2(2q + 2\lfloor 2q^{1/2} \rfloor)^{1/2} \rceil}. \tag{12}$$

If $q \geq 4$ is even and $\lfloor 2q^{1/2} \rfloor$ is even, then

$$A(q^3) \geq \frac{q + \lfloor 2q^{1/2} \rfloor - 1}{3 + \lceil 2(2q + 2\lfloor 2q^{1/2} \rfloor - 2)^{1/2} \rceil}. \tag{13}$$

A number q is called special if p divides $\lfloor 2q^{1/2} \rfloor$ or q can be represented in one of the forms $n^2 + 1$, $n^2 + n + 1$, $n^2 + n + 2$ for some integer n. They also proved that if $q \geq 11$ is odd, $\lfloor 2q^{1/2} \rfloor$ is even, and q is not special, then

$$A(q^3) \geq \frac{2q + 4\lfloor q^{1/2} \rfloor}{5 + \lceil 2(2q + 4\lfloor q^{1/2} \rfloor + 1)^{1/2} \rceil}. \tag{14}$$

Recently Temkine [19] extended Serre's lower bound (3) to

Theorem 1.5 *There exists an effective constant c such that*

$$A(q^r) \geq cr^2 \log q \frac{\log q}{\log r + \log q}. \tag{15}$$

It is also shown in [19] that $A(3) \geq \frac{8}{17} = 0.4705\ldots$ and $A(5) \geq \frac{8}{11} = 0.7272\ldots$, thus improving the corresponding bounds given in [10].

In this paper we employ class field towers to improve aforementioned lower bounds for $A(q)$ and to compute $A(p)$ for small primes p. We also give an alternative proof of Theorem 1.5 with an explicit and improved constant c. Finally, we present a lower bound for the l-rank of the S-divisor class group, similar to the corresponding result from [10]. More precisely, our results are as follows.

By using the explicit construction of ray class fields of function fields via rank one Drinfeld modules we prove the following generalisation of Theorem 1.3.

Theorems 3.3 *Let q be an odd prime power. Let r be an odd integer at least 3 and s be a positive integer relatively prime to r. Let $F/\mathbb{F}_q$ be a global function field and let N be the largest integer with the property that $B_s \geq N$ and $B_r > \lfloor (3 + \lceil 2(2N+1)^{1/2} \rceil)/(r-2) \rfloor$. Further suppose that $h(F\mathbb{F}_{q^r})/h(F)$ is odd. Then we have*

$$A(q^{rs}) \geq \frac{4Ns}{4g(F) + \left\lfloor \frac{3 + \lceil 2(2N+1)^{1/2} \rceil}{r-2} \right\rfloor + \lceil 2(2N+1)^{1/2} \rceil}. \tag{16}$$

By $\mathrm{f}(q) = \mathrm{O}(\mathrm{g}(q))$ we mean that there is a constant $M > 0$ such that $|\mathrm{f}(q)| \leq M|\mathrm{g}(q)|$ for all sufficiently large q. Immediate consequences of the above theorem are the following two corollaries.

Corollary 3.4 *Let q be an odd prime power. Let r be an odd integer at least 3 and s be a positive integer relatively prime to r. Let F be the rational function field $\mathbb{F}_q(x)$ and suppose that*

$$B_r > \left\lfloor (3 + \lceil 2(2B_s + 1)^{1/2} \rceil)/(r-2) \right\rfloor .$$

Then we have

$$A(q^{rs}) \geq \frac{\sqrt{2}(r-2)}{r-1}\sqrt{s}q^{s/2} + \mathrm{O}(1). \tag{17}$$

For $r < s < 2r$ the conditions of this corollary are satisfied for all q sufficiently large and the bound above improves the bound (6), which gives $A(q^{rs}) \geq \frac{\sqrt{2}}{2}q^{s/2} + \mathrm{O}(1)$.

Taking F to be the rational function field and $s = 1$, one gets the following improvement of (6) for $r \geq 5$.

Corollary 3.5 *Let q be an odd prime power. Then for any odd integer $r \geq 3$ we have*

$$A(q^r) \geq \frac{4q+4}{\left\lfloor \frac{3 + \lceil 2(2q+2)^{1/2} \rceil}{r-2} \right\rfloor + \lceil 2(2q+3)^{1/2} \rceil}. \tag{18}$$

A better lower bound for $A(q)$ with q even is derived from the following generalisation of Theorem 1.3.

Theorem 3.6 *Let $F/\mathbb{F}_q$ be a global function field of characteristic p. Let r be an odd integer at least 3 and s be a positive integer relatively prime to r. Let N be the largest integer such that $B_s \geq N$ and $B_r > \left\lfloor \frac{6+2\lceil 2\sqrt{2pN} \rceil}{r-1} \right\rfloor$. If $h(F\mathbb{F}_{q^r})/h(F)$ is not divisible by p, then*

$$A(q^r) \geq \frac{pNs}{pg(F) - p + 2(p-1)\left(3 + \lceil 2\sqrt{pN} \rceil\right)}. \tag{19}$$

Corollary 3.7 *Let q be a power of 2. Let r be an odd integer at least 3 and s be a positive integer relatively prime to r. Let F be the rational function field $\mathbb{F}_q(x)$. Suppose that*

$$B_r(F) > \left\lfloor \frac{6 + 2\left\lceil 4\sqrt{B_s(F)} \right\rceil}{r-1} \right\rfloor .$$

Then we have

$$A(q^{rs}) \geq \frac{\sqrt{2}}{4}\sqrt{s}q^{s/2} + \mathrm{O}(1). \tag{20}$$

For $r < s < 2r$ the conditions of this corollary are satisfied for all even q sufficiently large and the bound above improves the bound (7), which gives $A(q^{rs}) \geq \frac{\sqrt{2}}{4}q^{s/2} + \mathrm{O}(1)$.

By applying Theorem 3.6 to Deligne-Lusztig curves in characteristic 2, we obtain the following bound which improves (7), (12) and (13).

Theorem 3.8 *Let q be a power of 2. For $r \geq 5$ odd and all q sufficiently large we have*

$$A(q^r) \geq \frac{2q^2}{\sqrt{2q}(q-1) + 2\lceil 2\sqrt{2q} \rceil + 4}. \tag{21}$$

For $r = 3$ and all q sufficiently large we have

$$A(q^3) \geq \frac{2q^2}{\sqrt{2q}(q-4) + 8\lceil\sqrt{2}q\rceil + 16}. \tag{22}$$

The same ideas involved in the proof of the lower bound of $A(q^3)$ for q even can be used to prove the following bounds which improve the bounds of Corollary 1.4 and the bound (14) for characteristics 3, 5, and 7.

Theorem 3.12 *Let q be a power of $p = 3$, 5 or 7. Then for all q sufficiently large we have*

$$A(q^3) \geq \frac{2(q^2+p^2)}{\sqrt{pq}(q-p^2) + 4p(p-1)\lceil\sqrt{q^2/p+p}\rceil + 10p^2 - 12p}. \tag{23}$$

All of the above lower bounds for $A(q^r)$ are good for large q. The next result, which is a generalisation of the bound (3), is better for r large. Theorem 1.5 is a consequence of this.

Theorems 3.14 and 3.15 *Let $0 < \theta < 1/2$. Then for all sufficiently large odd q^r we have*

$$A(q^r) \geq \frac{((\lfloor\theta r \log q\rfloor - 3)^2 - 4)r}{2(\lceil 2\log r/\log q\rceil + 1)(\lfloor\theta r\log q\rfloor + 1) - 6}. \tag{24}$$

For all sufficiently large even q^r we have

$$A(q^r) \geq \frac{(\lfloor\theta r \log q\rfloor - 2)^2\, r}{4(\lceil 2\log r/\log q\rceil + 1)(\lfloor\theta r\log q\rfloor + 1) - 8}. \tag{25}$$

Using Tate cohomology, Niederreiter and Xing obtained a lower bound for the l-rank of the S-divisor class group Cl_S (see Proposition 4.1). In section 4 we present a proof of the following similar result.

Proposition 4.2 *Let $F/\mathbb{F}_q$ be a global function field and K a finite abelian extension of F. Let T be a finite nonempty set of places of F and S the set of places of K lying over those in T. If at least one place in T splits completely in K, then for any prime l we have*

$$d_l Cl_S \geq \sum_P d_l G_P - (|T| - 1 + d_l\mathbb{F}_q^*) - d_l G, \tag{26}$$

where $G = \mathrm{Gal}(K/F)$, G_P is the inertia subgroup at the place P of F, and $d_l X$ denotes the l-rank of an abelian group X. The sum is extended over all places P of F.

It is easily shown that this lower bound coincides with that of Niederreiter and Xing. The proof of the bound, which uses narrow ray class fields, reveals that the lower bound is really a lower bound of the l-rank of $\mathrm{Gal}(K'/K)$, where K' is the maximal subfield of the S-Hilbert class field of K which is an abelian extension of F. Finally, in section 4, lower bounds for $A(p)$ for small primes p are computed. We obtain $A(7) \geq 9/10$, $A(11) \geq 12/11 = 1.0909\ldots$ and $A(13) \geq 4/3$ and $A(17) \geq 8/5$.

2 Background on class field theory

2.1 Hilbert class fields

We recall, without proof, some basic facts about Hilbert class fields. The reader is referred to [15] for more details. Let $K/\mathbb{F}_q$ be a global function field with full constant field $\mathbb{F}_q$. Let S be a finite nonempty set of places of K and O_S the *S-integral ring* of K, i.e., O_S consists of all elements of K that have no poles outside S. Denote by O_S^* the group of units in O_S. If S consists of just one element P, then we write O_P and O_P^* for O_S and O_S^*. The *S-Hilbert class field* H_S of K is the maximal unramified abelian extension of K (in a fixed separable closure of K) in which all places in S split completely. The galois group of H_S/K, denoted by Cl_S, is isomorphic to the class group of O_S (see [15]); its order is the class number $h(O_S)$. If $S = \{P\}$ consists of one element, then $h(O_S) = dh(K)$ with $d = \deg P$ and $h(K)$ the divisor class number of K.

Now we define the *S-class field tower* of K. Let K_1 be the S-Hilbert class field H_S of K and S_1 the set of places of K_1 lying over those in S. Recursively, we define K_i to be the S_{i-1}-Hilbert class field of K_{i-1} for $i \geq 2$ and S_i to be the set of places of K_i lying over those in S_{i-1}. Then we get the *S-class field tower* of K: $K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots$. The tower is infinite if $K_i \neq K_{i-1}$ for all $i \geq 1$. The following proposition, known to Serre and proved by Schoof in [14], provides a sufficient condition for a class field tower to be infinite. It is a basic tool for our work, and it leads to the stated lower bound for $A(q)$. For a prime l and an abelian group B, denote by $d_l B$ the l-rank of B.

Proposition 2.1 *[14] Let $K/\mathbb{F}_q$ be a global function field of genus $g(K) > 1$ and let S be a nonempty set of places of K. Suppose that there exists a prime l such that*

$$d_l Cl_S \geq 2 + 2\left(d_l O_S^* + 1\right)^{1/2}. \tag{27}$$

Then K has an infinite S-class field tower. Furthermore if S consists of only rational places, then

$$A(q) \geq \frac{|S|}{g(K) - 1}.$$

The l-rank of O_S^* can be determined. Dirichlet's unit theorem asserts that $O_S^* \simeq \mathbb{F}_q^* \times \mathbf{Z}^{|S|-1}$, and therefore

$$d_l O_S^* = \begin{cases} |S| & \text{if } l|(q-1), \\ |S| - 1 & \text{otherwise.} \end{cases}$$

2.2 Narrow ray class fields

Since the explicit constructions of ray class fields via Drinfeld modules of rank 1 will be used, we recall the results and basic definitions. For more information the reader may consult [6], [15] and [5]. We shall follow the same notation as [12].

Let $F/\mathbb{F}_q$ be a global function field. We distinguish a place ∞ of F and let A be the subring of F consisting of all the functions which are regular away from ∞. Then the Hilbert class field H_A of F with respect to A is the maximal unramified abelian extension of F (in a fixed separable closure of F) in which the place ∞ splits completely. The galois group of H_A/F is isomorphic to the fractional ideal class group $\mathrm{Pic}(A)$ of A. If the degree of ∞ is 1 then the degree $[H_A : F]$ is the divisor class number $h(F)$ of F.

We fix a sign function sgn and let ϕ be a rank 1 sgn normalised Drinfeld A-module over H_A. The additive group of the algebraic closure $\overline{H_A}$ of H_A forms an A-module

under the action of ϕ. For any nonzero integral ideal M of A, the M-torsion module $\Lambda(M) = \{u \in \overline{H_A} : \phi_M(u) = 0\}$ is a cyclic A-module which is isomorphic to the A-module A/M and has $\Phi_q(M) := |(A/M)^*|$ generators, where $(A/M)^*$ is the group of units of the ring A/M. Let $\mathcal{I}(A)$ be the fractional ideal group of A and let $\mathcal{I}_M(A)$ be the subgroup of fractional ideals in $\mathcal{I}(A)$ prime to M. Define the quotient group $\mathrm{Pic}_M(A) = \mathcal{I}_M(A)/\mathcal{R}_M(A)$, where $\mathcal{R}_M(A)$ is the subgroup consisting of all principal ideals bA with $\mathrm{sgn}(b) = 1$ and $b \equiv 1 \bmod M$.

The field $F_M = H_A(\Lambda(M))$ generated by the elements of $\Lambda(M)$ over H_A is called the narrow ray class field of F modulo M. The extension F_M is unramified away from ∞ and the prime ideals in A which divide M. In fact, the maximal subfield in which ∞ splits completely is the ray class field of F with conductor M. We summarize below the main results from [6] which will be used later in the paper.

Proposition 2.2 *Let $F_M = H_A(\Lambda(M))$ be the narrow ray class field of F modulo M. Then:*
1. *F_M/F is an abelian extension and there is an isomorphism $\sigma : \mathrm{Pic}_M(A) \to \mathrm{Gal}(F_M/F)$ given by $\sigma_I\phi = I * \phi$ for any ideal I in A prime to M, and $\lambda^{\sigma_I} = \phi_I(\lambda)$ for any generator λ of the cyclic A-module $\Lambda(M)$. Moreover for any ideal I in A prime to M, the corresponding Artin automorphism of F_M/F is σ_I.*
2. *the muliplicative group $(A/M)^*$ is isomorphic to $\mathrm{Gal}(F_M/H_A)$ by means of $b \mapsto \sigma_{bA}$, where $b \in A$ is prime to M and satisfies $\mathrm{sgn}(b) = 1$.*
3. *both the decomposition group and the inertia group of F_M/F at ∞ are isomorphic to the multiplicative group $\mathbb{F}_q^*$.*
4. *if M decomposes into the product $M = \prod_{i=1}^t P_i^{e_i}$ of distinct prime ideals in A with $e_i \geq 1$, then F_M is the composite of the fields $H_A(\Lambda(P_1^{e_1}))$, $H_A(\Lambda(P_1^{e_2}))$, ..., $H_A(\Lambda(P_t^{e_t}))$. The order of the inertia group of F_M/F at P_i is $\Phi_q(P_i^{e_i})$, $i = 1, 2, \ldots, t$.*

3 General lower bounds for $A(q^r)$

Recall that $B_r(F)$ or simply B_r denotes the number of places of degree r in a function field F. The following estimate of the size of B_r was proved in [18] (Corollary V.2.10).

Proposition 3.1 *For a global function field $F/\mathbb{F}_q$ we have*

$$\left| B_r - \frac{q^r}{r} \right| \leq \left(\frac{q}{q-1} + 2g(F)\frac{q^{1/2}}{q^{1/2}-1} \right) \frac{q^{r/2}-1}{r} < (2 + 7g(F))\frac{q^{r/2}}{r}, \tag{28}$$

where $g(F)$ is the genus of F.

By $\mathrm{f}(q) = \mathrm{O}(\mathrm{g}(q))$ we mean that there is a constant $M > 0$ such that $|\mathrm{f}(q)| \leq M|\mathrm{g}(q)|$ for all sufficiently large q. Thus Proposition 3.1 implies that $B_r(\mathbb{F}_q(x)) = q^r/r + \mathrm{O}(q^{r/2})$.

3.1 Lower bounds for $A(q^r)$ with q odd

We start by proving a general theorem from which several improvements on lower bounds will be derived. Narrow ray class fields are used to construct infinite towers of function fields over $\mathbb{F}_{q^r}$.

For an odd integer $r \geq 3$ denote by F_r the extension of F by the constant field $\mathbb{F}_{q^r}$. Let s be a positive integer relatively prime to r. Then all the places of degree s in F

can be viewed naturally as degree s places of F_r. As in section 2.2, let A_r be the subring of F_r consisting of elements which are regular outside a chosen place ∞. Any place Q of degree r decomposes into a product of r prime ideals of degree 1 in A_r. In case no confusion can arise, we denote both the ideal $Q \cdot A$ and $Q \cdot A_r$ simply by Q. Thus $(A_r/Q)^* = (A_r/Q \cdot A_r)^*$ can be regarded as a subgroup of $\mathrm{Pic}_Q(A_r) = \mathrm{Pic}_{Q\cdot A_r}(A_r)$ in a canonical way.

As described in [12], the group $\mathrm{Pic}_Q(A)$ can also be viewed as a subgroup of $\mathrm{Pic}_Q(A_r)$ in a natural way. This is explained in the language of algebraic curves as follows. Let C be an algebraic curve over $\mathbb{F}_q$ with function field F. If we view C as a curve over $\overline{\mathbb{F}}_q$, then a divisor D on $C/\overline{\mathbb{F}}_q$ is a divisor of F if and only if D is $\mathbb{F}_q$-rational, that is, invariant under the action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Hence $\mathrm{Pic}_Q(A)$ can be described as the group of all $\mathbb{F}_q$-rational divisors on $C/\overline{\mathbb{F}}_q$ prime to Q and ∞, from which we factor out the group of all divisors $(c)_0$ with $c \in F$, $\mathrm{sgn}(c) = 1$, and $c \equiv 1 \bmod Q$ where $(c)_0$ is the divisor corresponding to the principal ideal cA. Since $\mathrm{Pic}_Q(A_r)$ has a similar description it follows that $\mathrm{Pic}_Q(A)$ is a subgroup of $\mathrm{Pic}_Q(A_r)$ in a natural way.

We will use the following result from [11].

Lemma 3.2 *Given a place Q of degree r of F, let $E_r = H_{A_r}(\Lambda(Q \cdot A_r))$ be the narrow ray class field of F_r modulo $Q \cdot A_r$. Let L be the subfield of E_r/F_r fixed by the subgroup $\mathrm{Pic}_Q(A)$ of $\mathrm{Gal}(E_r/F_r)$, and let K/F_r be the maximal unramified extension of F_r in L. Then the degree of the extension K/F_r is $h(F_r)/h(F)$.*

Let L be as in this lemma. Observe that a degree s place of $F_r/\mathbb{F}_{q^r}$ different from ∞ splits completely in L/F_r if and only if its Artin automorphism is contained in $\mathrm{Pic}_Q(A)$, and this happens if and only if the restriction of this place to $F/\mathbb{F}_q$ is a place of degree s. This fact will be used repeatedly.

Theorem 3.3 *Let q be an odd prime power. Let r be an odd integer at least 3 and s be a positive integer relatively prime to r. Let $F/\mathbb{F}_q$ be a global function field and let N be the largest integer such that $B_s \geq N$ and $B_r > \lfloor (3 + \lceil 2(2N+1)^{1/2} \rceil)/(r-2) \rfloor$. Further suppose that $h(F_r)/h(F)$ is odd. Then we have*

$$A(q^{rs}) \geq \frac{4Ns}{4g(F) + \left\lfloor \frac{3+\lceil 2(2N+1)^{1/2}\rceil}{r-2} \right\rfloor + \lceil 2(2N+1)^{1/2} \rceil}. \tag{29}$$

Proof: Put $n = \lfloor (3 + \lceil 2(2N+1)^{1/2} \rceil)/(r-2) \rfloor$ and let $Q_1, \ldots, Q_{n+1}$ be $n+1$ distinct places of degree r in F. Then each Q_i decomposes into a product $Q_i A_r = \prod_{j=1}^{r} Q_{ij}$ of r distinct prime ideals of degree one in A_r. For each i consider the narrow ray class field $E_r^{(i)} = H_{A_r}(\Lambda(Q_i))$ of F_r modulo Q_i. We use the abbreviations $h = h(F)$ and $h_r = h(F_r)$ for the remainder of the proof.

Let I_i be the inertia group of $E_r^{(i)}/F_r$ at ∞ and L_i the subfield of $E_r^{(i)}/F_r$ fixed by the subgroup $I_i \cdot \mathrm{Pic}_{Q_i}(A)$ of $\mathrm{Gal}(E_r^{(i)}/F_r)$. Since $|\mathrm{Pic}_{Q_i}(A)| = h(q^r-1)$, $|I_i| = q^r - 1$ and $|I_i \cap \mathrm{Pic}_{Q_i}(A)| = q-1$, it follows that $|I_i \cdot \mathrm{Pic}_{Q_i}(A)| = h(q^r-1)^2/(q-1)$. Hence $[L_i : F_r] = (h_r/h)(q-1)(q^r-1)^{r-2}$. The order of the inertia group of Q_{ij} in L_i/F_r divides $|(A_r/Q_{ij})^*| = q^r - 1$ for each $1 \leq j \leq r$, and therefore the inertia groups of $Q_{i3}, \ldots, Q_{ir}$ in L_i/F_r generate a subgroup G_i of $\mathrm{Gal}(L_i/F_r)$ of order dividing $(q^r-1)^{r-2}$. Let J_i be the subfield of L_i/F_r fixed by G_i, then $(h_r/h)(q-1)$ divides the degree of the extension J_i/F_r. The only possible ramified places in L_i/F_r are Q_{i1} and Q_{i2}.

Let $K_{i\,2}$ be a quadratic extension of F_r in L_i. (The reason for our choice of notation will become clear.) The only possible ramified places in $K_{i\,2}/F_r$ are Q_{i1} and Q_{i2}. On

the other hand, since h_r/h is odd, by Lemma 3.2, the field $K_{i\,2}$ is not contained in the maximal unramified extension of F_r in the subfield of $E_r^{(i)}$ fixed by $\mathrm{Pic}_{Q_i}(A)$. In other words, $K_{i\,2}/F_r$ is ramified. Thus at least one of the places Q_{i1}, Q_{i2} is ramified in $K_{i\,2}/F_r$. It is impossible for exactly one of these places to ramify in $K_{i\,2}/F_r$, for otherwise the Hurwitz genus formula would yield $2g(K_{i\,2})-2 = 2(2g(F_r)-2)+(2-1)\cdot 1$, contradicting the integrality of $g(K_{i\,2})$. Since $[K_{i\,2} : F_r] = 2$ and q^r is odd, $K_{i\,2}/F_r$ is a Kummer extension and we can write $K_{i\,2} = F_r(y_{i\,2})$, where $y_{i\,2}^2$ equals an element $u_{i\,2} \in F_r$. Since Q_{i1} and Q_{i2} are the only places of F_r that ramify in $K_{i\,2}$, it follows that for each place P of F_r, the valuation at P of $u_{i\,2}$, noted $v_P(u_{i\,j})$, is odd only when $P = Q_{i1}, Q_{i2}$.

Thus, by the above argument, for $1 \le i \le B_r$ and $2 \le j \le r-1$ we can form extensions $K_{i\,j} = F_r(y_{i\,j})$, where

$$y_{i\,j}^2 = u_{i\,j}$$

and in $K_{i\,j}/F_r$ the only two places that ramify are $Q_{i\,1}$ and $Q_{i\,j}$ so that the $u_{i\,j}$ have the property that $v_P(u_{i\,j})$ is odd only when $P = Q_{i1}, Q_{ij}$.

Let K'_j denote the compositum of the fields $K_{i\,j'}$ for $2 \le j' \le r-1$ and $j' \ne j$. Observe that $K_{i\,j} \cap K'_j = F_r$ because the place Q_{ij} is totally ramified in $K_{i\,j}/F_r$ but unramified in K'_j/F_r.

Before going further, we introduce more notation. Put $A = 3 + \lceil 2\sqrt{2N+1}\rceil$. Let t_1 be the integer $A - n(r-2)$. Thus $0 \le t_1 < r-2$. If $t_1 = 0$, set $t = 0$; if $t_1 > 0$ and t_1 is even, set $t = t_1$; otherwise set $t = t_1 + 1$. Define the sets

$$Z = \{(i,j) |\, 1 \le i \le n, 2 \le j \le r-1\} \cup \{(n+1,j) |\, 2 \le j \le t\},$$

where the second set is empty if $t = 0$ and

$$Z' = Z \cup \{(i,1) |\, (i,2) \in Z\}.$$

Form the extensions

$$K = F_r(\{y_{i\,j} |(i,j) \in Z\}).$$

and $L = F_r(y)$ with

$$y^2 = \prod_{(i,j)\in Z} u_{i\,j}(x). \tag{30}$$

The galois group of K/F_r is elementary abelian of exponent 2.

Since y^2 equals a product of some of the $y_{i\,j}^2$'s, it follows that L is a subfield of K. Observe from construction that if Z contains one pair (i,j), then it contains an odd number of pairs with the first component i. Consequently the places Q_{ij} with $(i,j) \in Z'$ are ramified in K/F_r with ramification index 2 by repeated application of Abhyankar's Lemma (see [18] chapter III). The same happens in the extension L/F_r. Therefore the extension K/L is unramified.

Let T' be a set of N places in F of degree s and T the set of N places in F_r which lie above those in T'. Then from the remarks preceding this theorem we know that all the places in T split completely in L/F_r. Let S' denote the $2N$ places in L which lie above the places in T. Now K/L is an unramified abelian extension in which the places in S' split completely. Moreover we have $d_l Cl_{S'} \ge d_l \mathrm{Gal}(K/L) = (n(r-2)+t)-1$. Since

$$n(r-2)+t-1 \ge n(r-2)+t_1-1 = 2+2\sqrt{2N+1} = 2+2\sqrt{|S'|+1},$$

it follows from Proposition 2.1 that L has an infinite S'-Hilbert class field tower.

By the Hurwitz genus formula we have,

$$\begin{aligned} 2g(L)-2 &= 2(2g(F_r)-2)+n(r-1)+t \\ &= 4g(F)+n-4+n(r-2)+t \\ &\leq 4g(F)+n-4+A+1 \\ &= 4g(F)+\left\lfloor \frac{3+\lceil 2(2N+1)^{1/2}\rceil}{r-2} \right\rfloor + \lceil 2(2N+1)^{1/2}\rceil. \end{aligned}$$

Passing to the constant field extension $L\mathbb{F}_{q^s}$, each place of degree s in S' splits into s places of degree 1 in $L\mathbb{F}_{q^s}$ and it is easily seen that $L\mathbb{F}_{q^s}$ has an infinite S-Hilbert class field tower where S is the set of those places of $L\mathbb{F}_{q^s}$ which lie above those in S'. We thus get, again by Proposition 2.1, that

$$\begin{aligned} A(q^{rs}) &\geq \frac{|S|}{g(L\mathbb{F}_{q^s})-1} = \frac{|S'|s}{g(L)-1} \\ &\geq \frac{4Ns}{4g(F)+\left\lfloor \frac{3+\lceil 2(2N+1)^{1/2}\rceil}{r-2} \right\rfloor + \lceil 2(2N+1)^{1/2}\rceil}, \end{aligned}$$

as desired.□

When applied to rational function fields, the theorem above yields the following lower bounds.

Corollary 3.4 *Let q be an odd prime power. Let r be an integer at least 3 and s be a positive integer relatively prime to r. Let F be the rational function field $\mathbb{F}_q(x)$. Suppose that*

$$B_r > \left\lfloor \left(3+\lceil 2(2B_s+1)^{1/2}\rceil\right)/(r-2)\right\rfloor.$$

Then we have

$$A(q^{rs}) \geq \frac{\sqrt{2}(r-2)}{r-1}\sqrt{s}q^{s/2}+\mathrm{O}(1). \tag{31}$$

For $r < s < 2r$ the conditions of Corollary 3.4 are satisfied for all q sufficiently large and the bound (31) improves the bound (6) which gives $A(q^{rs}) \geq \frac{\sqrt{2}}{2}q^{s/2}+\mathrm{O}(1)$.

Taking F to be the rational function field and $s=1$, one gets the following bound which improves (6) for $r \geq 5$.

Corollary 3.5 *Let q be an odd prime power. Then for any odd integer $r \geq 3$ we have*

$$A(q^r) \geq \frac{4q+4}{\left\lfloor \frac{3+\lceil 2(2q+2)^{1/2}\rceil}{r-2} \right\rfloor + \lceil 2(2q+3)^{1/2}\rceil}. \tag{32}$$

We remark that in the case that F is the rational function field $\mathbb{F}_q(x)$, the function fields K_{ij}, and hence L, of Theorem 3.3 can be explicitly defined. See [8] for the details.

By using similar ideas as in the proof of Theorem 3.3 one can prove the next theorem. Instead of using the modulus Q, we use Q^2. Moreover Artin-Schreier extensions are used instead of Kummer extensions.

Theorem 3.6 *Let $F/\mathbb{F}_q$ be a global function field of characteristic p. Let r be an odd integer at least 3 and s be a positive integer relatively prime to r. Let N be the largest integer such that $B_s \geq N$ and $B_r > \left\lfloor \frac{6+2\lceil 2\sqrt{2pN}\rceil}{r-1} \right\rfloor$. If $h(F\mathbb{F}_{q^r})/h(F)$ is not divisible by p, then*

$$A(q^r) \geq \frac{pNs}{pg(F)-p+2(p-1)\left(3+\lceil 2\sqrt{pN}\rceil\right)}. \tag{33}$$

One obtains similar corollaries as before.

3.2 Lower bounds for $A(q^r)$ with q even

We start with a consequence of Theorem 3.6 for the case of even q.

Corollary 3.7 *Let q be a power of 2. Let r be an odd integer at least 3 and let s be a positive integer relatively prime to r. Let F be the rational function field $\mathbb{F}_q(x)$. Suppose that*

$$B_r > \left\lfloor \frac{6 + 2\left\lceil 4\sqrt{B_s}\right\rceil}{r-1} \right\rfloor.$$

Then we have

$$A(q^{rs}) \geq \frac{\sqrt{2}}{4}\sqrt{s}q^{s/2} + \mathrm{O}(1). \qquad (34)$$

For $r < s < 2r$ the conditions of Corollary 3.7 are satisfied for all q sufficiently large and the bound (34) improves the bound (7), which gives $A(q^{rs}) \geq \frac{\sqrt{2}}{4}q^{s/2} + \mathrm{O}(1)$.

Letting $s = 1$, we obtain the following result which is similar to the bound (9) of Theorem 1.3.

Theorem 3.8 *Let q be a power of 2. Let $F/\mathbb{F}_q$ be a global function field with N rational places. Suppose that $B_r > \left\lfloor \frac{6+2\lceil 2\sqrt{2N}\rceil}{r-1} \right\rfloor$ and that the ratio of class numbers $h(F\mathbb{F}_{q^r})/h(F)$ is not divisible by 2. Then*

$$A(q^r) \geq \frac{N}{g(F) + \left\lceil 2\sqrt{2N}\right\rceil + 2}. \qquad (35)$$

Next we use this theorem to prove a lower bound for $A(q^r)$ which improves the bound (7).

Lemma 3.9 *Let $F/\mathbb{F}_q$ be a function field with at least one place of degree r and more than one rational place. Then $h(F_r)/h(F)$ divides the class number $h(O_S)$, where S consists of all but one rational places in F (viewed in F_r).*

Proof: Let Q be a place of degree r in F. Denote by ∞ the rational place of F not contained in S and define the ring A_r as before. Let $E_r = H_{A_r}(\Lambda(Q \cdot A_r))$ be the narrow ray class field of F_r modulo $Q \cdot A_r$. Let L be the subfield of E_r/F_r fixed by the subgroup $\mathrm{Pic}_Q(A)$ of $\mathrm{Gal}(E_r/F_r)$, and let K/F_r be the maximal unramified extension of F_r in L. Then, from the remarks preceding Theorem 3.3, all places in S split completely in K/F_r and, from Lemma 3.2, the degree of the extension K/F_r is $h(F_r)/h(F)$. On the other hand the degree of the maximal unramified abelian extension of F_r in which all the places in S split completely is $h(O_S)$ (see section 2.1). Hence $h(F_r)/h(F)$ divides $h(O_S)$.□

We will use the following result proved by Rosen [15].

Proposition 3.10 *Let L/K be a galois extension with degree a power of a prime l. Let S be a finite nonempty set of places of K. Suppose that every place in S splits completely in L and that at most one place of K ramifies in L. If S' is the set of primes of L which lie above those in S, then $l|h(O_{S'})$ implies $l|h(O_S)$.*

Theorem 3.11 *Let q be a power of 2. For $r \geq 5$ odd and q sufficiently large we have*

$$A(q^r) \geq \frac{2q^2+2}{\sqrt{2q}(q-1) + 2\lceil 2\sqrt{2q^2+2}\rceil + 4}.$$

For $r=3$ and q sufficiently large we have

$$A(q^3) \geq \frac{2q^2+8}{\sqrt{2q}(q-4)+8\lceil\sqrt{2q^2+8}\rceil+16}.$$

PROOF: Set $K=\mathbb{F}_q(x)$ and $K_r=\mathbb{F}_{q^r}(x)$. Write $q=2^{2m+1}=2q_0^2$ and define the extension $L=K(y)$ by

$$y^q+y=x^{q_0}(x^q+x).$$

Then L has degree q over K, it is totally ramified at ∞ and totally split at all other places of degree 1. Thus L has $N=q^2+1$ rational places. As computed in [4], L has genus $q_0(q-1)$. Let $L_r=K_r(y)$.

Let $r\geq 3$ be an odd number. In order to apply Theorem 3.8 to the function field L, we must show that the number of places of degree r in L satisfies the condition $B_r(L) > \left\lfloor (6+2\lceil 2\sqrt{2N}\rceil)/(r-1)\right\rfloor = \left\lfloor (6+2\lceil 2\sqrt{2q^2+2}\rceil)/(r-1)\right\rfloor$. By Proposition 3.1 we have $B_r(L) > (1/r)(q^r-(7/\sqrt{2})q^{\frac{r+3}{2}}+(7/\sqrt{2})q^{\frac{r+1}{2}}-2q^{\frac{r}{2}})$, hence the desired condition is satisfied for $r\geq 5$ and q sufficiently large. The extension L_r/K_r satisfies the conditions of Proposition 3.10 with $l=2$. Since $h(K_r)=1$, it follows from Proposition 3.10 and Lemma 3.9 that $h(L_r)/h(L)$ is odd.

Thus by Theorem 3.8, for $r\geq 5$ and all q sufficiently large we get

$$\begin{aligned} A(q^r) &\geq \frac{N}{g(L)+\left\lceil 2\sqrt{2N}\right\rceil+2} \\ &= \frac{2q^2+2}{\sqrt{2q}(q-1)+2\lceil 2\sqrt{2q^2+2}\rceil+4}. \end{aligned}$$

Next we consider the case $r=3$. Assume $q\geq 4$. Let M be a subfield of L of degree $q/4$ over K. Then this extension is totally ramified at ∞ and totally split at all other places of degree 1. Thus M has $N=q^2/4+1$ rational places. Next we compute the genus $g(M)$ of M. From Theorem 2.1 of [4] we have $g(M)=\sum_{i=1}^t E_i$ where E_1, E_2, ...,E_t ($t=q/4-1$) are the intermediate extensions $K\subseteq E_i\subseteq M$ with $[E_i:K]=2$. It follows from the proof of Proposition 1.2 of [4] that all the E_i have genus $g(E_i)=q_0$. Thus $g(M)=q_0(q/4-1)$.

By (28) we have for q sufficiently large

$$\begin{aligned} B_3(M) &\geq \frac{q^3}{3}-\left(\frac{q}{q-1}+2g(M)\frac{q^{1/2}}{q^{1/2}-1}\right)\frac{q^{3/2}-1}{3} \\ &\geq \frac{q^3}{3}-(2+3g(M))\frac{q^{3/2}-1}{3} \\ &= \frac{q^3}{3}-(2+3q_0(q/4-1))\frac{q^{3/2}-1}{3} \\ &= \frac{1}{3}\left(1-\frac{\sqrt{18}}{8}\right)q^3+\mathrm{O}(q^{3/2}). \end{aligned}$$

Thus $B_3(M) > \left\lfloor 3+\lceil 2\sqrt{2N}\rceil\right\rfloor = \left\lfloor 3+\lceil 2\sqrt{q^2/2+2}\rceil\right\rfloor$ for all sufficiently large q.

As above, the ratio of class numbers $h(M\mathbb{F}_{q^r})/h(M)$ is odd. Thus by Theorem 3.8, for all q sufficiently large, we get

$$\begin{aligned} A(q^3) &\geq \frac{N}{g(M) + \left\lceil 2\sqrt{2N} \right\rceil + 2} \\ &= \frac{2q^2+8}{\sqrt{2q}(q-4) + 8\lceil \sqrt{2q^2+8} \rceil + 16}, \end{aligned}$$

as required.□

Remark: The same ideas involved in the proof of the lower bound of $A(q^3)$ for q even can be used to prove the following bounds which improves the bounds of Corollary 1.4 and the bound (14) for characteristics 3, 5, and 7.

Theorem 3.12 *Let q be a power of $p = 3$, 5 or 7. Then for all q sufficiently large we have*

$$A(q^3) \geq \frac{2(q^2+p^2)}{\sqrt{pq}(q-p^2) + 4p(p-1)\lceil \sqrt{q^2/p+p} \rceil + 10p^2 - 12p}.$$

3.3 Improvements of Serre's bound

Throughout this section all logarithms will be of base 2. First we assume that q is odd. Let $r > 0$ be an odd integer. Put $k = \mathbb{F}_q(x)$, $k_r = \mathbb{F}_{q^r}(x)$. Given $0 < \theta < 1/2$, let n be the largest odd integer which does not exceed $1 + \theta r \log q$. We choose n to be odd merely for the sake of a neater proof. Let $N_t = B_t(k)$ denote the number of monic irreducible polynomials of degree t over $\mathbb{F}_q$. Let m be the smallest integer such that $N_m \geq n$.

The lemma below shows that $m \leq \lceil 2\log r/\log q \rceil + 1$ for q^r sufficiently large.

Lemma 3.13 *If $M = \lceil 2\log r/\log q \rceil + 1$, then $n \leq N_M$ for all q^r sufficiently large.*

Proof: Applying Proposition 3.1 to $F = k$, we get $N_M > (q^M - 2q^{M/2})/M$. Now $q^M - 2q^{M/2} \geq q^{2\log r/\log q + 1} - 2q^{\log r/\log q + 1} = qr(r-2)$. Since $qr(r-2)/M \geq 2\frac{q(r-2)}{\log r + \log q} \cdot r\log q$, the desired result follows.□

As $n \leq N_m$, we may choose n distinct monic irreducible polynomials $P_1(x)$, $P_2(x)$, ..., $P_n(x)$ of degree m over $\mathbb{F}_q$. For $1 \leq i \leq n$ define the extensions $k(y_i)/k$ with $y_i^2 = P_i(x)$. Let H be the compositum of the fields $k(y_1), ..., k(y_n)$. Further define the extension $k(y)$ by $y^2 = P_1(x)P_2(x)\cdots P_n(x)$. It is clear that the extension H is an unramified abelian extension of $k(y)$ of exponent 2 and the Galois group has 2-rank equal to $n-1$. Note that our choice of n being odd ensures that the place ∞ of k does not ramify in the extension $H/k(y)$. By Proposition 3.1, the number of degree r places B_r of H satisfies

$$B_r > \frac{q^r}{r} - (2 + 7g(H))\frac{q^{r/2}}{r}, \tag{36}$$

where $g(H)$ is the genus of H. Using the Hurwitz genus formula, we get $g(k(y)) - 1 = (mn + \epsilon - 4)/2$ and $g(H) = 2^{n-2}(mn+\epsilon-4)+1$, where ϵ is 1 if m is odd and 0 otherwise.

Now let P' be a place of degree r in H and let P be the place of $k(y)$ which lies below P'. Then $r = \deg P' = f(P'|P)\deg P$, where $f(P'|P)$ is the order of the decomposition group $G(P'|P)$, which is cyclic of order at most 2. Since r is odd, we have $f(P'|P) = 1$. Consequently the place P splits completely in the extension $H/k(y)$ and $\deg P = r$.

Thus each degree r place of H divides a degree r place of $k(y)$ which splits completely in $H/k(y)$. Consequently the number of degree r places of $k(y)$ which split completely in $H/k(y)$ is $B_r/[H:k(y)] = B_r/2^{n-1}$. From (36) we have

$$B_r/2^{n-1} > \frac{q^r}{2^{n-1}r} - \left(\frac{9}{2^{n-1}} + \frac{7}{2}(mn-3)\right)\frac{q^{r/2}}{r}.$$

As it is easily checked that

$$\frac{q^r}{2^{n-1}r} - \left(\frac{9}{2^{n-1}} + \frac{7}{2}(mn-3)\right)\frac{q^{r/2}}{r} \geq \left(\frac{n-3}{2}\right)^2 - 1$$

for all sufficiently large q^r, we can choose a set S' of $((n-3)/2)^2 - 1$ places of degree r of $k(y)$ which split completely in $H/k(y)$. Since $d_2 Cl_{S'} \geq n-1 = 2 + 2\sqrt{|S'|+1}$, we have by Proposition 2.1 that $k(y)$ has an infinite S'-Hilbert class field tower. Passing to the constant field extension $k_r(y)$, each place of degree r in $k(y)$ splits into r places of degree 1 in $k_r(y)$ and it is easily seen that $k_r(y)$ has an infinite S-Hilbert class field tower, where S is the set of those places of $k_r(y)$ which lie above those in S'. We thus get, again by Proposition 2.1, that

$$\begin{aligned}
A(q^r) &\geq \frac{|S|}{g(k_r(y))-1} = \frac{|S'|r}{g(k(y))-1} = 2((n-3)/2)^2-1)r/(mn+\epsilon-4) \\
&\geq ((n-3)^2-4)r/(2mn-6) \\
&\geq \frac{((\lfloor\theta r\log q\rfloor - 3)^2-4)r}{2(\lceil 2\log r/\log q\rceil + 1)(\lfloor\theta r\log q\rfloor + 1) - 6}
\end{aligned}$$

for all sufficiently large q^r. We have proved

Theorem 3.14 *Let $0 < \theta < 1/2$. Then for all sufficiently large odd q^r we have*

$$A(q^r) \geq \frac{((\lfloor\theta r\log q\rfloor - 3)^2-4)r}{2(\lceil 2\log r/\log q\rceil + 1)(\lfloor\theta r\log q\rfloor + 1) - 6}. \tag{37}$$

For q even the proof is essentially the same so we omit the details. The extensions $k(y_i)/k$ in this case are Artin-Schreier extensions defined by $y_i^2 + y_i = 1/P_i(x)$ and the extension $k(y)/k$ is defined by $y^2 + y = \sum_i 1/P_i(x)$. Also in this case, n need not be odd. The lower bound we get in this case is approximately half that of the q odd case.

Theorem 3.15 *Let $0 < \theta < 1/2$. Then for all sufficiently large even q^r we have*

$$A(q^r) \geq \frac{(\lfloor\theta r\log q\rfloor - 2)^2\, r}{4(\lceil 2\log r/\log q\rceil + 1)(\lfloor\theta r\log q\rfloor + 1) - 8}. \tag{38}$$

As the right hand side of (37) is at least $\frac{r\log q}{2}\cdot\frac{\theta^2 r^2(\log q)^2 - 8\theta r\log q + 12}{\theta r\log q(\log r + \log q) + \log r - 2\log q}$, which in turn is at least $\frac{\theta}{4}r^2(\log q)^2/(\log r + \log q)$ for all sufficiently large q^r, we see that the bound (37) implies the bound (15). The same is true for even q.

4 Lower bounds of $A(p)$ for small primes p

In view of the condition (27) in Proposition 2.1, it is important that we have good lower bounds for the l-rank of the S-divisor class group Cl_S. Niederreiter and Xing [10] proved the following lower bound.

Proposition 4.1 *Let F be a global function field and K/F a finite abelian extension. Let T be a finite nonempty set of places of F and S the set of places of K lying over those in T. Then for any prime l we have*

$$d_l Cl_S \geq \sum_P d_l G_P - d_l O_T^* - d_l G,$$

where $G = \mathrm{Gal}(K/F)$ and G_P is the inertia subgroup at the place P of F. The sum is extended over all places P of F.

Their proof uses Tate cohomology. Here we give another proof of this result assuming that at least one of the places in the set T splits completely, which is the case in applications. The proof below, which uses narrow ray class fields, reveals that the lower bound of Proposition 4.1 is really a lower bound of the l-rank of the Galois group of the maximal subfield of the S-Hilbert class field of K which is an abelian extension of F. If we remove the condition that a place of T splits completely in K/F, then the proof below can be easily modified to obtain a lower bound which is one less.

Proposition 4.2 *Let $F/\mathbb{F}_q$ be a global function field and K/F a finite abelian extension. Let T be a finite nonempty set of places of F and S the set of places of K lying over those in T. If at least one place in T splits completely in K, then for any prime l we have*

$$d_l Cl_S \geq \sum_P d_l G_P - (|T| - 1 + d_l \mathbb{F}_q^*) - d_l G,$$

where $G = \mathrm{Gal}(K/F)$, G_P is the inertia subgroup at the place P of F. The sum is extended over all places P of F.

Remark: Observe that $d_l O_T^* = |T| - 1 + d_l \mathbb{F}_q^*$ so that the bound coincides with the one of Proposition 4.1.

Proof of Proposition 4.2: We continue with the notation introduced in section 2.2. Obviously, we may assume that the extension K/F is ramified. Denote by ∞ a place in T which splits completely in K. Write A for the ring of elements in F regular outside ∞. Let M be the conductor of the extension K/F. Then M is the smallest modulus for which K is contained in the narrow ray class field F_M.

Since all the field extensions involved are abelian, we may speak of the decomposition group or inertia group of places in the base field without specifying a corresponding place above. Let G''_P be the inertia group of a place P of F in the extension F_M/F. Now for any place P' of K which lies above a place P in F, the inertia group of P' in the extension F_M/K is $G''_P \cap \mathrm{Gal}(F_M/K)$, which is independent of the choice of P'. We denote the group $G''_P \cap \mathrm{Gal}(F_M/K)$ by G'_P. Observe that G''_∞ is contained in $\mathrm{Gal}(F_M/H_A)$ and $\mathrm{Gal}(F_M/K)$. In particular, $G'_\infty = G''_\infty$.

If J is the fixed field of G''_P, then G_P is isomorphic to $\mathrm{Gal}(F_M/J \cap K)/\mathrm{Gal}(F_M/K)=$ $[G''_P \mathrm{Gal}(F_M/K)]/\mathrm{Gal}(F_M/K)$, which is isomorphic to $G''_P/G''_P \cap \mathrm{Gal}(F_M/K) = G''_P/G'_P$. In other words, $G_P \cong G''_P/G'_P$.

Suppose that M has prime decomposition $M = P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t}$, where P_1, P_2, ..., P_t are prime ideals of A and $e_1, e_2, \ldots, e_t \geq 1$. Let $G' = G'_{P_1} \cdots G'_{P_t}$ and $G'' = G''_{P_1} \cdots G''_{P_t}$. Then $G'' = \mathrm{Gal}(F_M/H_A)$ (cf. [6], [10]) so that $G''_\infty \subseteq G''$. Let L be the fixed field of $G'G'_\infty$ in the extension F_M/F. We have

$$d_l \mathrm{Gal}(L/F) \quad = \quad d_l \mathrm{Pic}_M(A)/\mathrm{Gal}(F_M/L)$$

$$
\begin{aligned}
&\geq d_l G''/G'_\infty G' \\
&= d_l\,(G''/G')\,/\,(G'_\infty G'/G') \\
&\geq d_l G''/G' - d_l G'_\infty G'/G' \\
&= \sum_{i=1}^{t} d_l G_{P_i} - d_l G'_\infty/G'_\infty \cap G' \\
&= \sum_{P} d_l G_P - d_l G'_\infty/G'_\infty \cap G', \qquad (39)
\end{aligned}
$$

where P ranges over all places of F.

Since ∞ splits completely in K, the field L contains K. Observe further that L/K is an unramified abelian extension. For each place $P \in T$ other than ∞, let H'_P be the decomposition group of any place of L dividing P, and let H_P be the intersection of H'_P with $\mathrm{Gal}(L/K)$. Denote by K' the fixed field of all H_P, $P \in T$ and $P \neq \infty$. Then K' is an unramified abelian extension of K in which all places in S split completely. In other words, K' is a subfield of the S-Hilbert class field of K. Since each H_P is cyclic, we have

$$d_l \mathrm{Gal}(L/K') \leq |T| - 1. \qquad (40)$$

We now have

$$
\begin{aligned}
d_l Cl_S &\geq d_l \mathrm{Gal}(K'/K) = d_l \mathrm{Gal}(L/K)/\mathrm{Gal}(L/K') \\
&\geq d_l \mathrm{Gal}(L/K) - d_l \mathrm{Gal}(L/K') \\
&\geq d_l \mathrm{Gal}(L/K) - (|T| - 1) \ \ (\text{by} \ \ (40)) \\
&\geq d_l \mathrm{Gal}(L/F) - d_l \mathrm{Gal}(K/F) - (|T| - 1) \\
&\geq \sum_P d_l G_P - (|T| - 1 + d_l G'_\infty/G'_\infty \cap G') - d_l G \ \ (\text{by} \ \ (39)) \\
&\geq \sum_P d_l G_P - (|T| - 1 + d_l G'_\infty) - d_l G.
\end{aligned}
$$

Since $G'_\infty \cong \mathbb{F}_q^*$, we are done.$\square$

Next we present lower bounds for $A(p)$ where $p = 7, 11, 13, 17$.

Theorem 4.3 *We have*

$$A(7) \geq 9/10$$

Proof: Let k be the rational function field $\mathbb{F}_7(x)$. Let $F = k(y)$ be the function field defined by

$$y^2 = Q(x) := x^6 + 2x^5 + 3x^4 + 3x^3 + x^2 + 1.$$

Then F/k is a Kummer extension in which all the rational places of k split completely. The only place ramifying in F/k is $Q(x)$ and by the Hurwitz genus formula $g(F) = 2$.

Let $K = k(z)$ be the function field defined by $z^2 = P(x)$ where

$$
\begin{aligned}
P(x) \ &= \ x(x+1)(x+2)(x^2+4x+6)(x^2+3x+6)(x^2+3x+1) \\
&\quad\ (x^2+6x+4)(x^2+6x+3)(x^2+2x+2)(x^2+4).
\end{aligned}
$$

Then K/k is a Kummer extension in which the places $x+3, x+4, x+5, x+6$ split completely and the ramified places are those in the set $R = \{x, x+1, x+2, x^2+4x+$

$6, x^2+3x+6, x^2+3x+1, x^2+6x+4, x^2+6x+3, x^2+2x+2, x^2+4, \infty\}$. Now, from the relations

$$\begin{aligned}
Q(x) &\equiv (3+2x)^2 \bmod x^2+4x+6 \\
Q(x) &\equiv (3+x)^2 \bmod x^2+3x+6 \\
Q(x) &\equiv (2+5x)^2 \bmod x^2+3x+1 \\
Q(x) &\equiv 1^2 \bmod x^2+6x+4 \\
Q(x) &\equiv (2+2x)^2 \bmod x^2+6x+3 \\
Q(x) &\equiv (3+x)^2 \bmod x^2+2x+2 \\
Q(x) &\equiv (2+5x)^2 \bmod x^2+4
\end{aligned}$$

it follows that all the places in the set R split completely in the extension F/k. Let T be the set of places of F lying over $x+2, x+3, x+4, x+5, x+6$ and S the set of places of FK lying over those in T. Then $|T| = 2\cdot 5 = 10$ and $|S| = 2+2\cdot 8 = 18$. By Proposition 4.1,

$$d_2 Cl_S \geq \sum_P d_2 G_P - |T| - d_2 G = 22 - 10 - 1 = 11,$$

where $G = \mathrm{Gal}(FK/F) \simeq \mathbf{Z}/2\mathbf{Z}$ and the sum runs over all places P of F. Since $11 \geq 2 + 2\sqrt{|S|+1}$, the condition (27) in Proposition 2.1 is satisfied. By the Hurwitz genus formula we have $2g(FK) - 2 = 2(2g(F)-2) + 2(4\cdot 1 + 7\cdot 2) = 40$, and so

$$A(7) \geq \frac{|S|}{g(FK)-1} = \frac{9}{10}.\square$$

Theorem 4.4 *We have*

$$A(11) \geq 12/11 = 1.0909\ldots$$

Proof: Put $k = \mathbb{F}_{11}(x)$. Let
$P(x) = (x^2+4x+2)(x^2+5x+7)(x^2+8x+9)(x^2+6x+7)(x^2+1)(x^2+3)(x^2+4)(x^2+5)(x^2+9)(x^2+10x+6)(x^2+6x+3)(x^2+x+1)(x^2+6x+2)(x^2+9x+5)(x^2+6x+10)(x^2+x+4)(x^2+x+6)(x^2+x+7)(x^2+x+8)(x^2+10x+4)(x^2+9x+4)(x^2+9x+10)(x^2+6x+1)(x^2+7x+9)$, which is a product of 24 irreducible polynomials of degree 2 over $\mathbb{F}_{11}$, call them $P_1(x)$,..., $P_{24}(x)$.

Consider the extension $k(y)$ defined by $y^2 = P(x)$. Now $k(y)$ is contained in the function field $F = k(y_1, \ldots, y_{24})$, where $y_i^2 = P_i(x)$ for $1 \leq i \leq 24$. Moreover the extension $F/k(y)$ is unramified, $\mathrm{Gal}(F/k(y)) \cong (\mathbb{Z}/2\mathbb{Z})^{23}$ and the place ∞ splits completely in F/k.

Now the the places in the set $T = \{x+\alpha | \alpha \in \mathbb{F}_{11}\} \cup \{\infty\}$ split completely in $k(y)/k$. Thus $k(y)$ is contained in the decomposition fields of the places in T . For each place $x+\alpha$ in T let G_α be the decomposition group of $x+\alpha$ in $\mathrm{Gal}(K/k)$. Then G_α is a cyclic subgroup of $\mathrm{Gal}(F/k(y))$.

Let H be the the subgroup of $\mathrm{Gal}(F/k(y))$ generated by the groups G_α. Since each group G_α is cyclic of order at most 2, it follows that $d_2 H \leq 11$. Let K' be the fixed field of H in F and let S be the set of places in $k(y)$ which lie above those in T. Then $K'/k(y)$ is an unramified abelian extension in which each place in S splits completely. We now have $d_2 Cl_S \geq d_2\mathrm{Gal}(K'/k(y)) \geq d_2\mathrm{Gal}(F/k(y)) - d_2\mathrm{Gal}(F/K') \geq 12 = 2+2\sqrt{|S|+1}$.

By the Hurwitz genus formula $g(k(y)) - 1 = \frac{1}{2}(-4 + 24\cdot 2) = 22$. Thus by Proposition 2.1 we have $A(11) \geq 24/22 = 1.0909\ldots.\square$

Theorem 4.5 *We have*

$$A(13) \geq 4/3 = 1.333\ldots$$

PROOF: Put $k = \mathbb{F}_{13}(x)$ and let $P(x) = x(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)(x-7)(x-9)$. Define the extension $k(y)/k$ by $y^2 = P(x)$. Then $g(k(y)) = 3$ and the only rational places that split completely in $k(y)/k$ are those in the set $T = \{x+2, x+3\}$. If S is the set of 4 places in $k(y)$ which lie above those in T, then by Proposition 4.1, we have $d_2 Cl_S \geq 10 - 2 - 1 = 7$. Since $7 > 2 + 2\sqrt{|S|+1}$, we have from Proposition 2.1 that $A(13) \geq |S|/(g(k(y)) - 1) = 4/3$ as required.$\square$

Likewise, by using the polynomial $P(x) = x(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)(x-7)(x-8)(x-9)(x-11)(x-12)(x-15)$ one can show that $A(17) \geq 8/5$.

5 Acknowledgements

We thank H. Niederreiter and A. Temkine for providing us with preprints of their papers related to the topic of this paper.

References

[1] A. GARCIA and H. STICHTENOTH, A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound, Invent. Math. **121** (1995), 211–222.

[2] A. GARCIA and H. STICHTENOTH, Asymptotically good towers of function fields over finite fields, C.R. Acad. Sci. Paris Sér. I Math. **322** (1996), 1067–1070.

[3] A. GARCIA and H. STICHTENOTH, On the asymptotic behaviour of some towers of function fields over finite fields, J. Number Theory **61** (1996), 248–273.

[4] A. GARCIA and H. STICHTENOTH, Elementary abelian p-extensions of algebraic function fields, Manuscripta math. **72**, 67–79 (1991).

[5] D. GOSS, Basic structures in function field arithmetic, Springer, Berlin, 1996.

[6] D.R. HAYES, A brief introduction to Drinfeld Modules, in: The arithmetic of function fields (D. Goss, D. R. Hayes, M. I. Rosen, eds.), de Gruyter, Berlin, 1992, pp. 1-32.

[7] Y. IHARA, Some remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), 721–724.

[8] W-C. W. Li, Various constructions of good codes. Proceedings of International Conference on Computational and Combinatorial Algebra, Hong Kong University, May 24-29, 1999, preprint.

[9] YU.I. MANIN, What is the maximum number of points on a curve over $\mathbb{F}_2$?, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), 715–720.

[10] H. NIEDERREITER and C.P. XING, Towers of global funtion fields with asymptotically many rational places and an improvement on the Gilbert-Varshamov bound. Math. Nachr. 195(1998), 171–186.

[11] H. NIEDERREITER and C.P. XING, Curve sequences with asymptotically many rational places, to appear in the AMS Summer Research Conference Proceedings (Seattle, 1997).

[12] H. NIEDERREITER and C.P. XING, Drinfeld modules of rank 1 and algebraic curves with many rational points. II ,Acta Arith., **81** (1997), 81-100.

[13] M. PERRET, Tours ramifiées infinies de corps de classes, J. Number Theory **38** (1991), 300–322.

[14] R. SCHOOF, Algebraic curves over $\mathbb{F}_2$ with many rational points, J. Number Theory **41** (1992), 6–14.

[15] M. ROSEN, The Hilbert class field in function fields, Exposition. Math., **5** (1987), 365-378.

[16] J.-P. SERRE, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, C.R. Acad. Sci. Paris Sér. I Math. **296** (1983), 397–402.

[17] J.-P. SERRE, Rational Points on Curves over Finite Fields, Lecture Notes, Harvard University, 1985.

[18] H. STICHTENOTH, Algebraic Function Fields and Codes, Springer, Berlin, 1993.

[19] A. TEMKINE, Hilbert class field towers of function fields over finite fields and lower bounds for $A(q)$, preprint (1999).

[20] M.A. TSFASMAN, S.G. VLĂDUT, and T. ZINK, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, Math. Nachr. **109** (1982), 21–28.

[21] S.G. VLĂDUT and V.G. DRINFEL'D, Number of points of an algebraic curve, Funct. Anal. Appl. **17** (1983), 53–54.

[22] T. ZINK, Degeneration of Shimura surfaces and a problem in coding theory, in Fundamentals of Computation Theory, L. BUDACH (ed.), Lecture Notes in Computer Science, Vol. **199**, Springer, Berlin, p. 503–511, 1985.